C L A I M S

What Is Claimed Is:

1. A secret key generation method for generating secret keys to be sent from a center to entities, comprising the step of:

generating said secret keys peculiar to said entities using pieces of information resulting from division of information specifying each of said entities.

2. An encryption method for use in a system in which a center sends to entities secret keys peculiar to the entities respectively, and each entity uses a secret key peculiar to itself that has been sent from the center when it encrypts plaintext to ciphertext, the encryption method comprising the steps of:

generating said secret keys peculiar to said entities using pieces of information resulting from division of information specifying each of said entities; and

encrypting plaintext to ciphertext using a common key generated using a component contained in the secret key peculiar to an entity that is a sender of the ciphertext, the component corresponding to one or more

pieces of information specifying another entity that is a destination of the ciphertext.

3. A cryptographic communications method for communications of information between entities wherein a plurality of centers are provided, each of which generates secret keys peculiar to the entities using divided pieces of information resulting from division of information specifying each of the entities; one entity generates a first common key using a first component contained in secret keys peculiar to the one entity sent from the centers, encrypts plaintext to ciphertext using the first common key and sends the ciphertext to another entity, the first component corresponding to one or more of the divided pieces of information specifying said another entity; and said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to the another entity sent from said centers, and decrypts said ciphertext to the original plaintext using the second common key, the second component corresponding to one or more of the divided pieces of information specifying the one entity.

4. A cryptographic communications method for communicating information between entities wherein:

secret keys peculiar to said entities are sent from a center to said entities;

one entity encrypts plaintext to ciphertext using a first common key derived from a first secret key peculiar to the one entity sent from said center and sends the ciphertext to another entity;

said another entity decrypts said ciphertext to the original plaintext using a second common key identical to the first common key, the second common key being derived from a second secret key peculiar to said another entity sent from said center, characterized in that;

a plurality of said centers are deployed;

each of said plurality of centers generates secret keys peculiar to said entities by adding random numbers peculiar to said entities to divided pieces of information resulting from division of information specifying each of said entities; and

each of said entities generates a common key using a component, contained in the secret key peculiar to that selfsame entity, corresponding to one or more of the divided pieces of information specifying an opposite entity.

5. The cryptographic communications method according to claim 4, wherein computation formulas for generating secret keys at said centers are as follows:

$$\overrightarrow{S_{i1}} \equiv g^{\alpha_{i1} H_1 \overrightarrow{[I_{i1}]}} \pmod{P}$$

$$\overrightarrow{S_{i2}} \equiv \alpha_{i2} H_2 \overrightarrow{[I_{i2}]} \pmod{P-1}$$

$$\vdots$$

$$\overrightarrow{S_{iK}} \equiv \alpha_{iK} H_K \overrightarrow{[I_{iK}]} \pmod{P-1}$$

where

vector s_{ij} is a secret key corresponding to j'th piece of divided information specifying entity i ($j = 1, 2, \ldots, K$)

[vector I_{ij}] is j'th piece of divided information specifying entity i;

P is a prime number;

K is number of divisions in the information specifying entity i;

g is primitive element for GF (P);

H_j is a symmetrical $2^M \times 2^M$ matrix made up of random numbers;

M is size of divisions in the information specifying entity i; and

α_{ij} is a personal secret random number for entity i (where $\alpha_{i1} \ldots \alpha_{iK} \equiv 1 \pmod{P-1}$).

6. The cryptographic communications method according to claim 5, wherein computation formulas for generating common keys at said entities are as follows:

$$
\begin{aligned}
K_{im} &\equiv \overrightarrow{S_{i1}}\,[\overrightarrow{I_{m1}}]^{\overrightarrow{S_{i2}}\,[\overrightarrow{I_{m2}}]\cdots\overrightarrow{S_{iK}}\,[\overrightarrow{I_{mK}}]} \\
&\equiv g^{\overrightarrow{\alpha_{i1}}\cdots\overrightarrow{\alpha_{iK}}H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]\cdots H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}]} \\
&\equiv g^{H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]\cdots H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}]} \pmod{P}
\end{aligned}
$$

where

K_{im} is common key generated by one entity i for another entity m; and

vector s_{ij} [vector I_{ij}] is a component contained in secret key vector s_{ij} of entity i, corresponding to divided piece of information specifying entity m.

7. A common key generator provided at entities in a cryptographic communications system for generating common keys to be used in processing to encrypt plaintext into ciphertext and in processing to decrypt ciphertext into plaintext, comprising:

storage means at each entity for storing secret keys peculiar to each respective entity produced for respective pieces of information resulting from division of information specifying each of said respective entities;

selection means for selecting components corresponding to pieces of information specifying opposite entities to be communicated with, from among the secret keys stored; and

means for generating said common keys using said components so selected.

8. A cryptographic communications system for reciprocally performing, between a plurality of entities, encrypting processing for encrypting plaintext that is information to be sent into ciphertext and decrypting processing for decrypting ciphertext so sent back into original plaintext; comprising:

a plurality of centers that generate secret keys peculiar to said entities using pieces of information resulting from division of information specifying each of said entities and that sends said secret keys to said entities; and

a plurality of entities each of which generates a common key employed mutually in said encryption and decryption processing when communicating with another entity, using a component contained in own secret key sent from the centers, the component corresponding to one or more pieces of information specifying said another entity.

9. A computer readable recording medium that stores a program that generates at entities involved in communications common keys used in processing to encrypt plaintext to ciphertext and in processing to decrypt said

ciphertext to said plaintext in a cryptographic communications system, comprising:

first program code means for causing said computer to select a component corresponding to one or more of divided pieces of information specifying one entity from a secret key peculiar to another entity; and

second program code means for causing said computer to generate said common keys using said components selected.

10. An encryption method comprising the steps of:

generating a first secret key peculiar to ciphertext sending entity using first divided specifying information and a second secret key peculiar to ciphertext receiving entity using second divided specifying information, the first divided specifying information being obtained by dividing specifying information of the ciphertext sending entity into a plurality of blocks and the second divided specifying information being obtained by dividing specifying information of the ciphertext receiving entity into a plurality of blocks;

generating a common key using a component contained in the first secret key, the component corresponding to second divided specifying information of the ciphertext receiving entity, the common key having a structure of at

least three layers and an exponent portion of the common key having a multi-layer structure; and

encrypting plaintext to ciphertext using the common key.

11. A secret key generation method comprising the step of:

generating secret keys peculiar to entities using divided specifying information resulting from division of information specifying said entities into a plurality of blocks; and wherein

secret key for a first block of divided specifying information has a multi-layer structure; and

each of secret keys for remaining blocks of divided specifying information has a single-layer structure.

12. An encryption method comprising the steps of:

generating secret keys peculiar to entities using divided specifying information resulting from division of information specifying said entities into a plurality of blocks; and

encrypting plaintext to ciphertext at one entity using a common key generated using a component contained in the secret key peculiar to the one entity, the component corresponding to divided specifying information

for another entity to which said ciphertext is to be sent, and wherein

secret key for first block of divided specifying information has a multi-layer structure; and

each of secret keys for remaining blocks of divided specifying information has a single-layer structure.

13. A cryptographic communications method for communications of information between entities wherein a plurality of centers are provided, each of which generates secret keys peculiar to the entities using divided specifying information resulting from division of information specifying each of the entities into a plurality of blocks; one entity generates a first common key using a first component contained in secret keys peculiar to the one entity sent from the centers, encrypts plaintext to ciphertext using the first common key and sends the ciphertext to another entity, the first component corresponding to one or more of the divided pieces of information specifying said another entity; and said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to the another entity sent from said centers, and decrypts said ciphertext to the original plaintext using the second common key, the second component corresponding to one or

more of the divided pieces of information specifying the one entity; secret keys for first block of divided specifying information have a multi-layer structure; and secret keys for remaining blocks of divided specifying information have a single-layer structure.

14. A secret key generation method for generating secret keys peculiar to entities using divided specifying information resulting from division of information specifying said entities into a plurality of blocks, wherein:

computation formulas for generating said secret keys are as follows:

$$\overrightarrow{S_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\overrightarrow{1}$$
$$\overrightarrow{S_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\overrightarrow{1}$$
$$\vdots$$
$$\overrightarrow{S_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\overrightarrow{1}$$
$$\vdots$$
$$\overrightarrow{S_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\overrightarrow{1}} \pmod{N}$$
$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{S_{i1}}} \pmod{N}$$
$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^2} \pmod{N}$$
$$\vdots$$
$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^t} \pmod{N}$$
$$\vdots$$
$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^T} \pmod{N}$$

where

vector s_{ij} is a secret key corresponding to j'th

divided specifying information for entity i ($j = 1, 2, \ldots, K$)

[vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i (where gcd (α_i, $\lambda(N)$) = 1 and $\lambda(\cdot)$ is Carmichael function);

N is such that $N = PQ$ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \ldots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of specifying information for entity i ($t = 0, 1, 2, \ldots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, then the expressions B = c^A and B = <A>^{c} represent (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = {a_{\mu\nu}}^{c}$

15. An encryption method wherein:

secret keys peculiar to entities are generated using divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks;

plaintext is encrypted to ciphertext at one entity using a common key generated using a component contained in the secret key peculiar to the one entity, the component corresponding to divided specifying information for another entity that is a destination of said ciphertext; and

computation formulas for generating said secret keys peculiar to said entities are as follows:

$$\overrightarrow{S_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\vec{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\vec{1}$$

$$\vdots$$

$$\overrightarrow{S_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\vec{1}$$

$$\vdots$$

$$\overrightarrow{S_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\vec{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\vec{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{S_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^T} \pmod N$$

where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i ($j = 1, 2, \ldots, K$)

[vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i

(where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is

Carmichael function);

N is such that N = PQ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \ldots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of specifying information for entity i (t = 0, 1, 2, ..., T);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}{}^{c}$

16. The encryption method according to claim 15, wherein computation formulas for generating said common keys are as follows:

$$g_{0im} = \overrightarrow{g_{i0}}\,[\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g}_{i1}[\overrightarrow{I}_{m1}]$$
$$\vdots$$
$$g_{tim} = \overrightarrow{g}_{it}[\overrightarrow{I}_{m1}]$$
$$\vdots$$
$$g_{Tim} = \overrightarrow{g}_{iT}[\overrightarrow{I}_{m1}]$$
$$x_{2im} = \overrightarrow{s}_{i2}[\overrightarrow{I}_{m2}]$$
$$\vdots$$
$$x_{jim} = \overrightarrow{s}_{ij}[\overrightarrow{I}_{mj}]$$
$$\vdots$$
$$x_{Kim} = \overrightarrow{s}_{iK}[\overrightarrow{I}_{mK}]$$

$$\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{{}_TC_t\, y_{im}^{(T-t)}} \\
&\equiv g^{\bar{\alpha}_i^T \sum_{t=0}^{T} {}_TC\, x_{1im}^{t}\, y_{im}^{T-t}} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+y_{im})^T} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+\cdots+x_{kim})^T} \\
&\equiv g^{\bar{\alpha}_i^T (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]+\beta_{iK})^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])+\lambda(N)\}^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])\}^T} \\
&\equiv g^{(H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \pmod N
\end{aligned}$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m, selected from own vector g_{it} for 1st block of information specifying entity i (t = 0, 1, 2, ..., T);

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component corresponding to vector I_{mj} for entity m, selected from own vector s_{ij} for j'th block of information specifying entity i (j = 2, 3, ..., K);

K_{im} is a common key generated by one entity i for another entity m; and

y_{im} is sum of (K-1) components x_{jim} (j = 2, 3, ..., K), that is, $y_{im} = x_{2im} + x_{3im} + \ldots + x_{Kim}$.

17. A cryptographic communications method for communications of information between entities, wherein

a plurality of centers are deployed, each of which generates secret keys peculiar to said entities using divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks, and sends the secret keys to the entities respectively;

one entity generates a first common key using a first component contained in secret keys peculiar to the one entity sent from the centers, encrypts plaintext to ciphertext using the first common key, and sends the ciphertext to said another entity, the first component corresponding to divided specifying information for another entity;

said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to said another entity sent from the centers, and decrypts said ciphertext using the second common key, the second

component corresponding to divided specifying information for the one entity; and

computation formulas for generating said secret keys at said centers are as follows:

$$\overrightarrow{S_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$
$$\overrightarrow{S_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$
$$\vdots$$
$$\overrightarrow{S_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$
$$\vdots$$
$$\overrightarrow{S_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T} \overrightarrow{1}} \pmod N$$
$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T} \overrightarrow{S_{i1}}} \pmod N$$
$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^2} \pmod N$$
$$\vdots$$
$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^t} \pmod N$$
$$\vdots$$
$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^T} \pmod N$$

where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i ($j = 1, 2, \ldots, K$)

[vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i (where gcd $(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is Carmichael function);

N is such that $N = PQ$ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \ldots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of information specifying entity i ($t = 0, 1, 2, \ldots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}{}^{C}$

18. The cryptographic communications method according to claim 17, wherein computation formulas for generating said common keys are as follows:

$$
\begin{aligned}
g_{0im} &= \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] \\
g_{1im} &= \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{tim} &= \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] \\
&\vdots \\
g_{Tim} &= \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}] \\
x_{2im} &= \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}] \\
&\vdots \\
x_{jim} &= \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}] \\
&\vdots \\
x_{Kim} &= \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]
\end{aligned}
$$

$$
\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{{}_{T}C_{t}\, y_{im}^{(T-t)}} \\
&\equiv g^{\bar{\alpha}_i^{T} \sum_{t=0}^{T} {}_{T}C\, x_{1im}^{t}\, y_{im}^{T-t}} \\
&\equiv g^{\bar{\alpha}_i^{T} (x_{1im}+y_{im})^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T} (x_{1im}+\cdots+x_{kim})^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T} (\alpha_i H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}]+\beta_{iK})^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T} \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])+\lambda(N)\}^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T} \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])\}^{T}} \\
&\equiv g^{(H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])^{T}} \pmod N
\end{aligned}
$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m, selected from own vector g_{it} for 1st block

of information specifying entity i ($t = 0, 1, 2, \ldots, T$);

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component corresponding to vector I_{mj} for entity m, selected from own vector s_{ij} for j'th block of information specifying entity i ($j = 2, 3, \ldots, K$);

K_{im} is a common key generated by one entity i for another entity m; and

y_{im} is sum of (K-1) components x_{jim} ($j = 2, 3, \ldots, K$), that is, $y_{im} = x_{2im} + x_{3im} + \ldots + x_{Kim}$.

19. A common key generator provided at entities in a cryptographic communications system for generating a common key to be used in processing to encrypt plaintext to ciphertext and in processing to decrypt ciphertext back to plaintext, comprising:

storage means for storing secret keys peculiar to said entities produced, according to computation formulas given below, for divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks;

selection means for selecting components corresponding to divided specifying information for

opposite entities to be communicated with, from the secret keys stored; and

means for generating said common keys, according to computation formulas given below, using said components so selected:

$$\overrightarrow{S_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \vec{1}$$
$$\overrightarrow{S_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \vec{1}$$
$$\vdots$$
$$\overrightarrow{S_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \vec{1}$$
$$\vdots$$
$$\overrightarrow{S_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \vec{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T} \vec{1}} \pmod{N}$$
$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T} \overrightarrow{S_{i1}}} \pmod{N}$$
$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^2} \pmod{N}$$
$$\vdots$$
$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^t} \pmod{N}$$
$$\vdots$$
$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^T} \pmod{N}$$

where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i ($j = 1, 2, \ldots, K$)

[vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i (where gcd $(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is Carmichael function);

N is such that $N = PQ$ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \ldots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of information specifying entity i ($t = 0, 1, 2, \ldots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}{}^c$

$$g_{0im} = \overrightarrow{g_{i0}}\,[\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}}\,[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}\,[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}\,[\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}\,[\overrightarrow{I_{m2}}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}}\,[\overrightarrow{I_{mj}}]$$

$$\vdots$$

$$x_{Kim} = \overrightarrow{s_{iK}}\,[\overrightarrow{I_{mK}}]$$

$$\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{{}_T C_t\, y_{im}^{(T-t)}} \\
&\equiv g^{\bar{\alpha}_i^T \sum_{t=0}^{T} {}_T C\, x_{1im}^{t}\, y_{im}^{T-t}} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+y_{im})^T} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+\cdots+x_{kim})^T} \\
&\equiv g^{\bar{\alpha}_i^T (\alpha_i H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}]+\beta_{iK})^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])+\lambda(N)\}^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])\}^T} \\
&\equiv g^{(H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])^T} \pmod N
\end{aligned}$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m, selected from own vector g_{it} for 1st block of information specifying entity i (t = 0, 1, 2, ..., T);

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component

corresponding to vector I_{mj} for entity m, selected from own vector s_{ij} for j'th block of information specifying entity i (j = 2, 3, ..., K);

K_{im} is a common key generated by one entity i for another entity m; and

y_{im} is sum of (K-1) components x_{jim} (j = 2, 3, ..., K), that is, $y_{im} = x_{2im} + x_{3im} + \ldots + x_{Kim}$.

20. A cryptographic communications system for reciprocally performing, between a plurality of entities, encryption processing for encrypting plaintext that is information to be sent into ciphertext and decryption processing for decrypting ciphertext so sent back into original plaintext, comprising:

a plurality of centers each of which generates secret keys peculiar to said entities, according to computation formulas given below, using divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks, and sends said secret keys to said entities; and

a plurality of entities each of which generates a common key mutually employed in said encryption and decryption processing when communicating with another

entity, according to computation formulas given below, using a component contained in own secret key sent from said centers, the component corresponding to divided specifying information for said another entity:

$$\overrightarrow{S_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1}\vec{1}$$
$$\overrightarrow{S_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2}\vec{1}$$
$$\vdots$$
$$\overrightarrow{S_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij}\vec{1}$$
$$\vdots$$
$$\overrightarrow{S_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK}\vec{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}\vec{1}} \pmod{N}$$
$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}\overrightarrow{S_{i1}}} \pmod{N}$$
$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^2} \pmod{N}$$
$$\vdots$$
$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^t} \pmod{N}$$
$$\vdots$$
$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}<\overrightarrow{S_{i1}}>^T} \pmod{N}$$

where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i ($j = 1, 2, \ldots, K$)

[vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i (where gcd $(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is Carmichael function);

N is such that $N = PQ$ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \ldots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of information specifying entity i ($t = 0, 1, 2, \ldots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}{}^{c}$

$$g_{0im} = \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}]$$

$$
\begin{aligned}
g_{1im} &= \overrightarrow{g_{i1}}\,[\overrightarrow{I_{m1}}] \\
&\;\vdots \\
g_{tim} &= \overrightarrow{g_{it}}\,[\overrightarrow{I_{m1}}] \\
&\;\vdots \\
g_{Tim} &= \overrightarrow{g_{iT}}\,[\overrightarrow{I_{m1}}] \\
x_{2im} &= \overrightarrow{s_{i2}}\,[\overrightarrow{I_{m2}}] \\
&\;\vdots \\
x_{jim} &= \overrightarrow{s_{ij}}\,[\overrightarrow{I_{mj}}] \\
&\;\vdots \\
x_{Kim} &= \overrightarrow{s_{iK}}\,[\overrightarrow{I_{mK}}]
\end{aligned}
$$

$$
\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{\,{}_TC_t\, y_{im}^{(T-t)}} \\
&\equiv g^{\bar{\alpha}_i^T \sum_{t=0}^{T} {}_TC x_{1im}^{t}\, y_{im}^{T-t}} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+y_{im})^T} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+\cdots+x_{kim})^T} \\
&\equiv g^{\bar{\alpha}_i^T (\alpha_i H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\beta_{i1}+\cdots+\alpha_i H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}]+\beta_{iK})^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])+\lambda(N)\}^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])\}^T} \\
&\equiv g^{(H_1[\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}]+\cdots+H_K[\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])^T} \pmod N
\end{aligned}
$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m, selected from own vector g_{it} for 1st block of information specifying entity i (t = 0, 1, 2, ..., T);

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component corresponding to vector I_{mj} for entity m, selected from own vector s_{ij} for j'th block

of information specifying entity i ($j = 2, 3, \ldots, K$);

K_{im} is a common key generated by one entity i for another entity m; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3, \ldots, K$), that is, $y_{im} = x_{2im} + x_{3im} + \ldots + x_{Kim}$.

21. A computer readable recording medium for storing a program that generates at entities involved in communications a common key mutually used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext back to said plaintext in a cryptographic communications system, comprising:

first program code means for causing said computer to select a component corresponding to divided specifying information of one entity that is a ciphertext recipient from a secret key peculiar to another entity that is a ciphertext sender, according to computation formulas given below, for each of divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks; and

second program code means for causing said computer to generate said common key, according to computation formulas given below, using said components selected:

$$\overrightarrow{S_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \vec{1}$$

$$\vdots$$

$$\overrightarrow{S_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \vec{1}$$

$$\vdots$$

$$\overrightarrow{S_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \vec{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T} \vec{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T} \overrightarrow{S_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^T} \pmod N$$

where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i ($j = 1, 2, \ldots, K$)

[vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i (where gcd (α_i, $\lambda(N)$) = 1 and $\lambda(\cdot)$ is

Carmichael function);

N is such that N = PQ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \ldots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of information specifying entity i (t = 0, 1, 2, ..., T);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions $B = c^A$ and $B = \langle A\rangle^c$ represent (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}{}^{c}$

$$g_{0im} = \overrightarrow{g_{i0}}\,[\overrightarrow{I_{ml}}]$$

$$g_{1im} = \overrightarrow{g_{i1}}\,[\overrightarrow{I_{ml}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}\,[\overrightarrow{I_{ml}}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}\,[\overrightarrow{I_{ml}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}\,[\overrightarrow{I_{m2}}]$$
$$\vdots$$
$$x_{jim} = \overrightarrow{s_{ij}}\,[\overrightarrow{I_{mj}}]$$
$$\vdots$$
$$x_{Kim} = \overrightarrow{s_{iK}}\,[\overrightarrow{I_{mK}}]$$

$$\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{{}_T C_t\, y_{im}^{(T-t)}} \\
&\equiv g^{\bar{\alpha}_i^T \sum_{t=0}^{T} {}_T C_t\, x_{1im}^{t}\, y_{im}^{T-t}} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+y_{im})^T} \\
&\equiv g^{\bar{\alpha}_i^T (x_{1im}+\cdots+x_{kim})^T} \\
&\equiv g^{\bar{\alpha}_i^T (\alpha_i H_1 [\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}] + \beta_{i1} + \cdots + \alpha_i H_K [\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}] + \beta_{iK})^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1 [\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}] + \cdots + H_K [\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}]) + \lambda(N)\}^T} \\
&\equiv g^{\bar{\alpha}_i^T \{\alpha_i (H_1 [\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}] + \cdots + H_K [\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])\}^T} \\
&\equiv g^{(H_1 [\overrightarrow{I_{i1}}]\,[\overrightarrow{I_{m1}}] + \cdots + H_K [\overrightarrow{I_{iK}}]\,[\overrightarrow{I_{mK}}])^T} \pmod{N}
\end{aligned}$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m, selected from own vector g_{it} for 1st block of information specifying entity i (t = 0, 1, 2, ..., T);

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component corresponding to vector I_{mj} for entity m, selected from own vector s_{ij} for j'th block of information specifying entity i (j = 2, 3, ..., K);

K_{im} is a common key generated by one entity i for another entity m; and

y_{im} is sum of (K-1) components x_{jim} (j = 2, 3,

..., K), that is, $y_{im} = x_{2im} + x_{3im} + \ldots + x_{Kim}$.

22. A computer data signal embodied in a carrier wave for generating at entities involved in communications common keys used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext to said plaintext in a cryptographic communications system, comprising:

first code segment for causing a computer to select a component corresponding to one or more of divided pieces of information specifying one entity from a secret key peculiar to another entity; and

second code segment for causing said computer to generate said common keys using said components selected.

23. A computer data signal embodied in a carrier wave for generating at entities involved in communications a common key mutually used in processing to encrypt plaintext to ciphertext and in processing to decrypt said ciphertext back to said plaintext in a cryptographic communications system, comprising:

first code segment for causing a computer to select a component corresponding to divided specifying information of one entity that is a ciphertext recipient from a secret key peculiar to another entity that is a

ciphertext sender, according to computation formulas given below, for each of divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks; and

second code segment for causing said computer to generate said common key, according to computation formulas given below, using said components selected:

$$\overrightarrow{S_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{S_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{S_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T} \overrightarrow{1}} \pmod N$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T} \overrightarrow{S_{i1}}} \pmod N$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^2} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^t} \pmod N$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T} < \overrightarrow{S_{i1}} >^T} \pmod N$$

where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i (j = 1, 2, ..., K)

[vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i (where gcd $(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is Carmichael function);

N is such that N = PQ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \ldots + \beta_{iK} = \lambda(N)$);

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of information specifying entity i ($t = 0, 1, 2, \ldots, T$);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii) and (iv) below, respectively.

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}{}^{C}$

$$g_{0im} = \overrightarrow{g_{i0}}\,[\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}}\,[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}\,[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}\,[\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}\,[\overrightarrow{I_{m2}}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}}\,[\overrightarrow{I_{mj}}]$$

$$\vdots$$

$$x_{Kim} = \overrightarrow{s_{iK}}\,[\overrightarrow{I_{mK}}]$$

$$
\begin{aligned}
K_{im} &\equiv \prod_{t=0}^{T} g_{tim}^{{}_{T}C_{t}\, y_{im}^{(T-t)}} \\
&\equiv g^{\bar{\alpha}_i^{T} \sum_{t=0}^{T} {}_{T}C\, x_{1im}^{t}\; y_{im}^{T-t}} \\
&\equiv g^{\bar{\alpha}_i^{T}\, (x_{1im}+y_{im})^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T}\, (x_{1im}+\cdots+x_{kim})^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T}\, (\alpha_i H_1[\overrightarrow{I_{i1}}]\, [\overrightarrow{I_{m1}}] + \beta_{i1} + \cdots + \alpha_i H_K[\overrightarrow{I_{iK}}]\, [\overrightarrow{I_{mK}}] + \beta_{iK})^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T}\, \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\, [\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}]\, [\overrightarrow{I_{mK}}]) + \lambda(N)\}^{T}} \\
&\equiv g^{\bar{\alpha}_i^{T}\, \{\alpha_i (H_1[\overrightarrow{I_{i1}}]\, [\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}]\, [\overrightarrow{I_{mK}}])\}^{T}} \\
&\equiv g^{(H_1[\overrightarrow{I_{i1}}]\, [\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}]\, [\overrightarrow{I_{mK}}])^{T}} \pmod{N}
\end{aligned}
$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m, selected from own vector g_{it} for 1st block of information specifying entity i (t = 0, 1, 2, ..., T);

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component corresponding to vector I_{mj} for entity m, selected from own vector s_{ij} for j'th block of information specifying entity i (j = 2, 3, ..., K);

K_{im} is a common key generated by one entity i for another entity m; and

y_{im} is sum of (K-1) components x_{jim} (j = 2, 3, ..., K), that is, $y_{im} = x_{2im} + x_{3im} + \ldots + x_{Kim}$.